

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION**

BEVERLY T. PETERS,
individually and on behalf of all
others similarly situated,

PLAINTIFF

v.

ST. JOSEPH SERVICES CORP.
d/b/a ST. JOSEPH HEALTH
SYSTEM and
ST. JOSEPH REGIONAL HEALTH
CENTER,

DEFENDANTS

CASE NO.: 3:14-cv-00114

JURY TRIAL DEMANDED

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANTS' RULE
12(b)(6) MOTION TO DISMISS

TABLE OF CONTENTS

NATURE OF THE CASE.....	1
BACKGROUND FACTS.....	2
STANDARD OF REVIEW.....	5
ARGUMENTS AND AUTHORITIES.....	6
A. Peters properly states a claim for St. Joseph’s violations of the Fair Credit Reporting Act (“FCRA”) (Counts I and II, Complaint ¶¶ 66-81).....	7
1. The Fair Credit Reporting Act, 15.U.S.C. §1681, et seq	8
2. St. Joseph is a consumer reporting agency under FCRA	10
3. St. Joseph’s “data furnishing” argument conflates the definition of a CRA with the Data Breach itself, and makes no sense	12
B. Peters properly states claims for St. Joseph’s FCRA violations Counts I and II, Complaint, ¶¶ 66-81), negligence (Count V, Complaint, ¶¶ 91-100), negligence per se (Count VI, Complaint, ¶¶ 101-105), breach of contract (Count VII, Complaint, ¶¶ 111-115), Violation of the Texas DTPA (Count IX, Complaint, 116-120), and breach of fiduciary duty (Count XI, Complaint, ¶¶ 127-137).....	15
C. Peters properly states claims for breach of contract and/or breach Of implied contract.....	16
1. Peters properly states her breach of contract claim (Count VII, Complaint ¶¶ 106-110).....	16
2. Peters properly states her breach of implied contract claim (Count VIII, Complaint ¶¶ 111-115)	19
D. Peters properly states her Texas Deceptive Trade Practices-	

	Consumer Protection Act (“DTPA”) claims (Count IX, Complaint ¶¶ 116-120).....	24
E.	Peters properly states her invasion of privacy claim (Count X, Complaint ¶¶ 121-126).....	24
F.	Peters properly alleges emotional distress	26
G.	Peters properly states her claims for negligence per se (Count VI, Complaint ¶¶ 101-105).....	27
H.	Peters properly states her claims for St. Joseph’s violations of the Texas Medical Practice Act (Count III, Complaint ¶¶ 86-90), and Breach of fiduciary duty (Count XI, Complaint, ¶¶ 127-137	28
I.	Peters properly states her breach of confidentiality claim (Count XII, Complaint, ¶¶ 138-141)	30

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Anderson v. Hannaford Bros.</i> , 659 F.3d 151 (1st Cir. 2011).....	21, 22
<i>Arbaugh v. Y&H Corp.</i> , 546 U.S. 500 (2006).....	15
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	6
<i>Barber v. Time, Inc.</i> , 159 S.W.2d 291 (Mo. 1942)	26
<i>Beaudry v. TeleCheck Services, Inc.</i> , 579 F.3d 702 (6th Cir. 2009)	14
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	6
<i>Biddle v. Warren Gen. Hosp.</i> , 715 N.E.2d 518 (Ohio 1999)	30
<i>Biederman's of Springfield, Inc. v. Wright</i> , 322 S.W.2d 892 (Mo. 1959)	26
<i>Causey v. Sewell Cad.–Chev., Inc.</i> , 394 F.3d 285 (5th Cir. 2004)	6
<i>Erickson v. Pardus</i> , 551 U.S. 89 (2007).....	6
<i>Gen. Universal Sys. v. HAL Inc.</i> , 500 F.3d 444 (5th Cir. 2007)	7, 12
<i>Grable & Sons Metal Prod., Inc. v. Darue Eng. & Mfg.</i> , 545 U.S. 308 (2005).....	28
<i>Harrison v. Williams Dental Group, P.C.</i> , 140 S.W.3d 912 (Tex. App.-Dallas 2004, no pet.)	20

<i>Haws & Garrett Gen. Contractors, Inc. v. Gorbett Bros. Welding Co.,</i> 480 S.W.2d 607 (Tex.1972).....	20
<i>Hollywood Fantasy Corp. v. Gabor,</i> 151 F.3d 203 (5th Cir. 1998)	20
<i>I.S. v. Washington University,</i> No. 4:11CV235SNLJ, 2011 WL 2433585 (E. D. Mo. June 14, 2011)	28
<i>Indus. Found. v. Texas Indus. Acc. Bd.,</i> 540 S.W.2d 668 (Tex. 1976), <i>cert. denied</i> , 430 U.S. 931 (1977).....	26
<i>Karl Rove & Co. v. Thornburgh,</i> 39 F.3d 1273 (5th Cir. 1994)	21
<i>McClung v. Wal-Mart,</i> 866 F. Supp. 306 (N.D. Tex. 1994)	23, 24
<i>Michaels Stores Pin Pad Litig.,</i> 830 F. Supp. 2d 518 (N.D. Ill. 2011).....	21
<i>Ori v. Fifth Third Bank,</i> 674 F. Supp. 2d 1095 (E.D. Wis. 2009)	10
<i>R.K. v. St. Mary’s Medical Center, Inc.,</i> 735 S.E.2d 715 (W.Va. 2012).....	28
<i>Richardson v. DSW, Inc.,</i> Case No. 05 C 4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005).....	21
<i>Rowe v. UniCare Life & Health Ins. Co.,</i> No. 09 C 2286, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010)	10
<i>Smith v. First Nat. Bank of Atlanta,</i> 837 F.2d 1575 (11th Cir. 1988)	12
<i>Star-Telegram, Inc. v. Doe,</i> 915 S.W.2d 471 (Tex. 1995)	25
<i>Texaco, Inc. v. Pennzoil Co.,</i> 729 S.W.2d 768 (Tex. App.-Houston [1st Dist.] 1987, writ ref’d n.r.e.).....	21

United States v. Whitfield,
590 F.3d 325 (5th Cir. 2009)7, 12

Washington v. CRC Credit Services, Inc.,
199 F.3d 263, 268-69 (5th Cir. 2000)14

Williams v. KCMO Broad. Div. Meredith Corp.,
472 S.W.2d 1 (Mo. App. 1971)26

Statutes

15 U.S.C. § 1681passim

28 U.S.C. § 136715

FED. R. CIV. P.1, 6, 31, 32

Fair Credit Reporting Act (FCRA)passim

Health Insurance Portability and Accountability Act of 1996 (HIPAA).....27, 28, 29

Texas Deceptive Trade Practices-Consumer Protection Act.....4, 15, 22, 23, 24

Texas Hospital Licensing Law.....29

Texas Medical Practice Act29

Other Authorities

Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV.
1426 (1982).....30

Brian C. Murchison, *Reflections on Breach of Confidence from the U.S.*
Experience.....30

Plaintiff Beverly T. Peters (“Peters”), on behalf of herself and all others similarly situated, files this response to the FED. R. CIV. P. 12(b)(6) Motion to Dismiss (“MTD”) (Doc.# 27) filed by Defendants St. Joseph Services Corporation d/b/a St. Joseph Health System and St. Joseph Regional Health Center (together, “St. Joseph”), and respectfully shows the following:

NATURE OF THE CASE¹

This is a consumer class action data breach lawsuit seeking redress for St. Joseph’s unauthorized disclosure of the highly confidential and personal information of Peters and approximately 405,000 similarly situated persons (*i.e.*, the Class Members) (the “Data Breach”). Unlike the typical consumer data breach case only involving personally identifiable information (“PII”)—such as, for example, names, addresses, Social Security numbers, and dates of birth—this case, more importantly, also involves protected health information (“PHI”)—such as, for example, medical diagnoses, medical treatments, prescribed medications, charts and other medical records. This is a medical data breach case.

Peters is a former St. Joseph patient. The Class Members are current and former St. Joseph patients, employees and some employees’ beneficiaries. Peters, on behalf of herself and Class Members, asserts thirteen (13) different causes of action. Rather than stepping up to the plate, taking responsibility for its conduct

¹ This section of this Response is taken from Peters’ allegations in Paragraphs 1-8 of her First Amended Class Action Complaint (the “Complaint”) (Doc. #22).

and the resulting Data Breach, and addressing the harm inflicted on its current and former patients and employees, St. Joseph asks the Court to dismiss this action. According to St. Joseph, there is no legal claim anywhere under which it is liable for the economic damages and other injury inflicted by the Data Breach. For the reasons set forth below, St. Joseph's MTD should be denied.

BACKGROUND FACTS

On February 4, 2014, St. Joseph announced that between December 16, 2013 and December 18, 2013, a server on its computer system storing patient and employee PII/PHI for several St. Joseph facilities granted unauthorized access to data thieves operating from China and elsewhere. Complaint, ¶41.

The infiltrated server contained the PII/PHI of Plaintiff and approximately 405,000 Class Members, which was disseminated by St. Joseph into the public domain and compromised. Complaint, ¶42. On information and belief, none of the disseminated and compromised PII/PHI was encrypted. *Id.* The Data Breach is one of the largest medical data breaches in the history of the United States. *Id.*

St. Joseph also announced it was belatedly "taking appropriate additional security measures to strengthen the security of its system," (*id.*), which are the PII/PHI data security measures, policies, procedures, protocols, and software and hardware systems it should already have instituted. Complaint, ¶43. Had such PII/PHI data security measures, policies, procedures, protocols, and software and

hardware systems been in place, functioning and properly monitored, the Data Breach never would have occurred. *Id.*

What's more, despite knowing about the Data Breach since at least December 18, 2013, St. Joseph did not announce it or commence notifying Peters and Class Members until February 4, 2014—almost seven weeks later. Complaint, ¶44. Had Peters and Class Members known about the Data Breach sooner, they could have taken certain defensive measures much earlier—such as changing financial account and payment card passwords and email addresses—to mitigate their injuries and damages. *Id.* St. Joseph's Data Breach notification delay, therefore, also substantially increased the risk of additional real and impending future economic damages and other actual harm to Peters and Class Members resulting from identity theft, identity fraud and/or medical fraud. *Id.*

During the intervening period between the Data Breach and the date the Data Breach notification letters were sent to Peters and Class Members, their unencrypted PII/PHI, on information and belief, was bought and sold several times on the robust international cyber black market—as evidenced by the identity theft, identity fraud and/or medical fraud Peters has already suffered—while they had no chance to take measures to protect its confidentiality. Complaint, ¶45.

Rather than getting out in front of the Data Breach and proactively offering Peters and Class Members real protection from identity theft, identity fraud and/or

medical fraud resulting from their compromised PII/PHI, St. Joseph only offered them one year of credit monitoring (Complaint, Exhibit A)—even though it is well known that data thieves routinely use stolen PII/PHI for longer than a year, and often wait more than a year to use stolen information until the conclusion of one year basic credit monitoring programs breached organizations typically offer. Complaint, ¶46. Even then, only a year of credit monitoring is woefully insufficient given the trove of unencrypted PII/PHI disseminated to the world in the Data Breach and the manipulation and machinations of cyber criminals. *Id.*

In truth, the actual post-Data Breach “PII/PHI protection services” allegedly offered by St. Joseph and at what price are remarkably indiscernible—which could be a violation of the Texas Deceptive Trade Practices-Consumer Protection Act in itself. Complaint, ¶47. At best, the proffered credit monitoring indirectly tracks identity theft; while it may reveal new credit accounts opened with the stolen information, it will do nothing to monitor unauthorized charges made to, for example, existing payment card accounts. *Id.* Notwithstanding St. Joseph’s promises, the offered “PII/PHI protection services,” in truth, are significantly less than advertised. *See* Complaint, ¶48, for the reasons why.

St. Joseph’s Data Breach notification letters (Complaint, Exhibit A) also are a less-than-subtle attempt to shift the burden and expense of the Data Breach to Peters and Class Members by, *inter alia*, encouraging them to (i) regularly

purchase their credit reports from the three major credit reporting agencies, (ii) contact law enforcement and/or government agencies if anything looks amiss in their financial/retail accounts, (iii) place fraud alerts on their credit reports, and (iv) place and/or lift freezes on their credit files, which must be done at each credit reporting agency at a cost of \$5 to \$20 each. Complaint, ¶49. All of these actions take time and money—which St. Joseph advised and encouraged Peters and Class Members to incur, but has not offered to pay. *Id.*

St. Joseph’s above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph’s failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Peters’ and Class Members’ PII/PHI, and caused them to suffer economic damages and other actual harm. Complaint, ¶54. *See also* Peters’ Response to St. Joseph’s Rule 12(b)(1) MTD, which she incorporates, by reference.

STANDARD OF REVIEW

Federal Rule of Civil Procedure 8(a)(2) provides that “[a] pleading that states a claim for relief must contain ... a short and plain statement of the claim showing that the pleader is entitled to relief.”

Rule 12(b)(6) authorizes a defendant to move to dismiss a complaint for failure to state a claim upon which relief may be granted. In considering a Rule 12(b)(6) motion, a district court must construe a complaint in the light most favorable to the plaintiff; the plaintiff's allegations must be taken as true. *Erickson v. Pardus*, 551 U.S. 89, 93–94 (2007). The district court's review is limited to the complaint allegations and any documents attached to a defendant's dismissal motion if the documents are referenced in the complaint and are central to the claims. *Causey v. Sewell Cad.–Chev., Inc.*, 394 F.3d 285, 288 (5th Cir. 2004).

To survive a motion to dismiss, a complaint must contain sufficient factual matter to “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). The plausibility standard, however, is not akin to a “probability requirement,” but rather, asks for more than a “possibility that a defendant has acted unlawfully.” *Twombly*, 550 U.S. at 556.

As discussed in greater detail below, Peters’ Complaint easily meets the Rule 8/*Iqbal*/*Twombly* pleading standard.

ARGUMENTS AND AUTHORITIES

Peters first notes that St. Joseph does not contest—and, therefore, waives—any arguments against her money had and received/assumpsit claim (Count XIII, Complaint, ¶¶ 142-146). *See, e.g., United States v. Whitfield*, 590 F.3d 325, 346

(5th Cir. 2009) (a party waives any argument it fails to make in its opening brief); *Gen. Universal Sys. v. HAL Inc.*, 500 F.3d 444, 454 (5th Cir. 2007) (even when an issue is mentioned in passing in a brief, a party waives the issue when it fails to present sufficient argument in support of its position in the brief).

A. Peters properly states a claim for St. Joseph’s violations of the Fair Credit Reporting Act (“FCRA”) (Counts I and II, Complaint, ¶¶ 66-81).

FCRA was enacted to require consumer reporting agencies “to adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the *confidentiality*, accuracy, relevancy, and *proper utilization* of such information.” 15 U.S.C. § 1681(b) (emphasis added). *See also* 15 U.S.C. § 1681(a)(4) (“[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a *respect for the consumer’s right to privacy.*”) (emphasis added).

By its above-described wrongful actions, inaction and/or omissions, and the resulting Data Breach, Peters alleges St. Joseph willfully and recklessly or, at the very least, negligently, violated FCRA. Complaint, ¶5.

Here, St. Joseph does not dispute it regularly engages in assembling or evaluating consumer credit information for the purpose of furnishing consumer reports to third parties. Rather, St. Joseph argues that Peters’ FCRA claim should be dismissed—as a matter of law—because (i) St. Joseph is not a “consumer

reporting agency” (“CRA”) under FCRA (MTD at 6-10), and, in any event, (ii) St. Joseph did not “furnish” data as that term is defined in the statute (MTD at 10-11).

St. Joseph is wrong on both points. Moreover, St. Joseph focuses only on Peters’ and Class Members’ PII—while totally ignoring its FCRA obligations to safeguard and protect their PHI. And, although couched as legal arguments, St. Joseph’s arguments, in truth, are factual arguments on the merits. But this is the pleading stage, and the Court must accept Peters’ alleged facts as true.

1. The Fair Credit Reporting Act, 15 U.S.C. §1681, *et seq.*

Under 15 U.S.C. § 1681a(f), a “consumer reporting agency” includes any organization which, for monetary fees or on a cooperative nonprofit basis, regularly engages in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing “consumer reports” to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

Under 15 U.S.C. § 1681a(d)(1), a “consumer report” is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be

used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.

“Consumer credit information” (PII) includes, *inter alia*, a person’s name, identification number (*e.g.*, Social Security number), marital status, physical address and contact information, educational background, employment, professional or business history, financial accounts and financial account history (*i.e.*, details of the management of the accounts), credit report inquiries (*i.e.*, whenever consumer credit information is requested from a credit reporting agency), judgments, administration orders, defaults, and other notices.

Under 15 U.S.C. § 1681a(i), “medical information” (PHI) is information or data, in any form or medium, created by or derived from a health care provider or the consumer, that relates to the (i) past, present, or future physical, mental, or behavioral health or condition of an individual, (ii) provision of health care to an individual, and (iii) payment for the provision of health care to an individual.

FCRA limits the dissemination of “consumer credit information” (PII) to certain well-defined circumstances and no other. 15 U.S.C. § 1681b(a). FCRA also specifically protects “medical information” (PHI). *See, e.g.*, 15 U.S.C. §1681a(d)(3) (“Restriction on sharing of medical information”); §1681b(g) (“protection of medical information”); §1681c(a)(6) (“Information excluded from consumer reports”).

2. St. Joseph is a consumer reporting agency under FCRA.

FCRA's definition of a CRA is broad. It is not limited to traditional credit bureaus, such as Experian, Equifax, or TransUnion—as St. Joseph suggests. *See, e.g., Rowe v. UniCare Life & Health Ins. Co.*, No. 09 C 2286, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010) (health insurance provider was a CRA under FCRA); *Ori v. Fifth Third Bank*, 674 F. Supp. 2d 1095, 1097–98 (E.D. Wis. 2009) (reseller was a CRA under FCRA).

St. Joseph's cited cases to the contrary suffer from pleading defects that do not exist here and/or are based on inapposite facts. Cutting through the string citations and superficial briefing, St. Joseph advances two arguments on this point.

St. Joseph first argues that entities utilizing consumer reports for “business, commercial, or professional purposes” are not CRAs under FCRA. MTD at 8. Although it does not carry the argument to conclusion, St. Joseph seems to infer that because Peters, as a consumer, gave St. Joseph her PII/PHI in connection with securing health care services—which are professional services—St. Joseph cannot be a CRA. This is absurd. While Peters and Class Members gave St. Joseph their PII/PHI in connection with securing health care services, St. Joseph—just like any other vendor of consumer goods and services—used the PII to get paid. The focus is not on how Peters and Class Members utilized the PII, but how St. Joseph utilizes it.

Nowhere does St. Joseph dispute it received, assembled and/or evaluated their “consumer credit information” and/or “medical information” protected by FCRA (*i.e.*, their PII/PHI) for the purpose of furnishing consumer reports to third parties. St. Joseph also does not dispute it used the means and/or facilities of interstate commerce to prepare, furnish and transmit consumer reports containing the PII/PHI to third parties—for the ultimate purposes of, *inter alia*, establishing Peters’ and Class Members’ eligibility for health care services, confirming whether such health care services were covered by their health insurance and/or securing payment for the provision of such health care services. Complaint, ¶74.

St. Joseph’s alleged use of Peters’ and Class Members’ PII for this purpose falls squarely within the confines of FCRA; to wit, information “bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.” Complaint, ¶ 69 (referencing 15 U.S.C. § 1681a(d)(1)). St. Joseph concedes, and waives any

opposition to, Peters’ FCRA claims pertaining to its wrongful and unauthorized disclosure of her PHI into the public domain by not addressing these claims.²

St. Joseph also argues it is not a CRA because “entities, like St. Joseph, that simply pass on information are not credit reporting agencies” (MTD at 9 (irrelevant citations omitted)), and further, “St. Joseph acquires information for one purpose, to facilitate providing healthcare services, and it is not a ‘consumer reporting agency.’” MTD at 10. But this is a fact-based argument to be explored and vetted during the discovery process, not addressed at the motion to dismiss stage. The Court’s consideration of St. Joseph’s MTD is based on the facts pled in Peters’ Complaint, which—when accepted as true—demonstrate that St. Joseph is a CRA under FCRA. St. Joseph has not, and cannot, demonstrate to the contrary.

3. St. Joseph’s “data furnishing” argument conflates the definition of a CRA with the Data Breach itself, and makes no sense.

Under 15 U.S.C. § 1681a(f), a CRA is defined to include any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information

² St. Joseph cites, but does not analyze or apply, *McCready* and *Ippolito* (MTD at 8)—which is of no consequence because they do not apply here in any event. St. Joseph also mentions, in passing, *Smith v. First Nat. Bank of Atlanta*, 837 F.2d 1575, 1579 (11th Cir. 1988), for the proposition that courts have held the terms “assemble and evaluate” to mean more than “receipt and retransmission of information.” That’s it, however. No analysis. No application to the pleadings in this case; just a stray comment. Thus, whatever points St. Joseph may have intended to make are waived. *See Whitfield* and *Gen. Universal Sys.*, *supra*.

or other consumer information for the purpose of *furnishing* “consumer reports” to third parties... .” (emphasis added). Thus, if a person—such as St. Joseph—is a CRA it is charged with protecting the PII/PHI entrusted to it.

Here, St. Joseph argues that since Peters’ PII/PHI was stolen by third parties, it did not “furnish” the PII/PHI to the data thieves and, therefore, it cannot be a CRA under FCRA. But FCRA does not require that a violation be the “data furnishing” event itself in order for there to be a violation of the statute. The Section 1681a(f) “data furnishing” provision is definitional—meaning, if St. Joseph regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing “consumer reports” to third parties, which St. Joseph does not dispute, it is a CRA under FCRA required to protect Peters’ and Class Members’ PII/PHI at all times pursuant to FCRA.

St. Joseph is a CRA under FCRA. St. Joseph did not protect Peters’ and Class Members’ PII/PHI as required by FCRA. St. Joseph violated FCRA. *Willingham* and *Holmes* (MTD at 11) are inapposite; they do not apply because they were pled differently or suffered from pleading defects that do not exist here.

In any event, St. Joseph’s argument ignores the ordinary meaning of the word “furnish,” which is to “supply” or “give.” *See Merriam-Webster Dictionary*.³

³ <http://www.merriam-webster.com/dictionary/furnish>.

Here, by virtue of St. Joseph's reckless, willful and negligent failure to safeguard and protect Peters' and Class Members' PII/PHI pursuant to FCRA, it "supplied" or "gave" the information to third parties—*i.e.*, St. Joseph "furnished" Peters' and Class Members' PII/PHI to the data thieves. *See, e.g.*, Complaint, ¶¶ 1, 4, 23, 48, 54, 57, 59, 85, 90, 100, 105, 118, 120, 126, 137, and 141 (referring to St. Joseph's unauthorized disclosure of the PII/PHI). *See also* Peters' compendium of Complaint allegations asserting St. Joseph's disclosure of her PII/PHI at Section H, *infra*, which Peters incorporates by reference.

4. Injunctive relief under FCRA.

St. Joseph argues that Peters does not state a valid claim for injunctive relief under FCRA, citing *Washington v. CRC Credit Services, Inc.*, 199 F.3d 263, 268-69 (5th Cir. 2000) (MTD at 11-12). However, in a more recent case, the Sixth Circuit, in *Beaudry v. TeleCheck Services, Inc.*, 579 F.3d 702, 709 (6th Cir. 2009), questioned the Fifth Circuit's ruling. Peters suggests the Sixth Circuit's holding is well reasoned and should be adopted, but at the same time, concedes the Fifth Circuit's present position on the matter. In any event, there are plenty of other grounds in Peters' Complaint on which injunctive relief may be granted.

5. Even if the Court dismisses Peters' FCRA claims, it should exercise supplemental jurisdiction over her state law claims.

St. Joseph next argues that without a FCRA claim, there is no federal question jurisdiction and, as such, all of Peters' state law claims should be dismissed.

(MTD at 12-14)—which is a surprising argument considering the waste of the Parties’ resources that would occur if they had to start over in state court after all of the work that has been done to date in this case.

St. Joseph’s argument, of course, assumes Peters’ FCRA claims will be dismissed even though St. Joseph does not articulate a cogent, well-reasoned basis for doing so. And, even if that occurs, the Supreme Court disagrees with St. Joseph’s position. *See Arbaugh v. Y&H Corp.*, 546 U.S. 500, 514 (2006) (“[W]hen a court grants a motion to dismiss for failure to state a federal claim, the court generally retains discretion to exercise supplemental jurisdiction, pursuant to 28 U.S.C. § 1367, over pendent state-law claims.”). Peters’ FCRA claims should not be dismissed, but if they are, the Court should retain this case.

B. Peters properly states claims for St. Joseph’s FCRA violations (Counts I and II, Complaint, ¶¶ 66-81), negligence (Count V, Complaint, ¶¶ 91-100), negligence *per se* (Count VI, Complaint, ¶¶ 101-105), breach of contract (Count VII, Complaint, ¶¶ 106-110), breach of implied contract (Count VIII, Complaint, ¶¶ 111-115), violation of the Texas DTPA (Count IX, Complaint, ¶¶ 116-120), and breach of fiduciary duty (Count XI, Complaint, ¶¶ 127-137).

St. Joseph next attacks these claims *en masse*, arguing for dismissal because Peters allegedly does not allege any actual, compensable damages. MTD at 14-16. St. Joseph is wrong. Throughout her Complaint, Peters repeatedly alleges economic damages and other actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii)

breach of the confidentiality of their PII/PHI, (iv) statutory damages under FCRA, (v) lost benefit of their bargains, (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vii) diminished value of the medical services they purchased from St. Joseph, and (viii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date. *See, e.g., id.* at ¶¶ 16-19, 54, 77, 81, 85, 90, 93, 100, 105, 120, 126, 137, 141, and 148.

Peters explains her damages in detail—including the FCRA statutory damages St. Joseph conveniently forgets—in her Response to St. Joseph’s Rule 12(b)(1) MTD, which she incorporates by reference.

C. Peters properly states claims for breach of contract and/or breach of implied contract.

1. Peters properly states her breach of contract claim (Count VII, Complaint, ¶¶106-110).

St. Joseph accurately states the elements of a breach of contract claim. MTD at 16. St. Joseph, however, does not dispute that Peters alleges all of the elements of her claim, but rather, string cites cases from other district courts—*Dyer*, *Trikas*, and *Northwest Airlines Privacy Litig.*—for the proposition that “online statements made by a company concerning privacy of data do not establish a binding contract.” MTD at 17.

All of St. Joseph's cited cases are distinguishable and do not apply here. None of them are data breach cases. None of the facts underpinning *Dyer*, *Trikas*, and *Northwest Airlines Privacy Litig.* are remotely close to the facts here. All of the cases speak in terms of "general statements" or "broad statements" of company policy—as opposed to the detailed and specific St. Joseph Privacy Notice that recognizes its *legal duty* to safeguard its patients' PHI. *See* Complaint, Exhibit B. Moreover, the court in *Trikas*, a summary judgment case, *specifically did not address* whether the Privacy Promise on defendant's website constituted a contract. *Id.*, 351 F.Supp.2d at 46.

As a condition to providing health care services, St. Joseph requires its patients to supply their detailed PII/PHI. Complaint, ¶33. St. Joseph also recognizes maintaining the confidentiality of its patients' PII/PHI is paramount:

Safeguarding patients' health information is *not only a legal requirement but also an important ethical obligation*. As a health care provider, St. Joseph and its staff are entrusted with clinical information regarding our patients. *We recognize that medical and billing records are highly confidential and must be treated with great respect and care* by all staff with access to this information. St. Joseph's policy regarding confidentiality of protected health care information reflects *our strong commitment to protecting the confidentiality of our patients' medical records and clinical information*.⁴

(emphasis added). *Id.*

⁴ *See* <http://www.st-joseph.org/body.cfm?id=461> (last visited March 25, 2014).

St. Joseph also makes certain representations, warranties and commitments to its patients in its Privacy Notice regarding the privacy of their PII/PHI. Complaint, ¶34 (citing Exhibit B). The Privacy Notice is posted in each St. Joseph facility (*id.* at 1) and on the St. Joseph website.⁵ *Id.* The Privacy Notice is also given to every St. Joseph patient—including Peters. Indeed, each St. Joseph patient must sign the Privacy Notice, acknowledging its existence and terms as a condition to receiving health care services. *Id.* at 3. Peters signed the Privacy Notice. Complaint, ¶34.

St. Joseph itemizes its privacy obligations in the Privacy Notice, making a firm commitment to uphold them; to wit, “St. Joseph is required by law to maintain the privacy of health information about you that can identify you (‘Protected Health Information’ or ‘PHI’), to provide you with this Notice of our legal duties and privacy practices with respect to your PHI, and to abide by the terms of the Notice currently in effect.” *Id.* at 1 (Complaint, ¶35).

The Privacy Notice lists specific, limited permissible purposes for which St. Joseph may use or disclose all or a portion of its patients’ PII/PHI without their authorization. *Id.* at 1-2 (Complaint, ¶36). For any purpose other than a listed purpose, a patient’s PHI may be used or disclosed only when authorized on an

⁵ See <http://www.st-joseph.org/workfiles/privacy.pdf> (last visited March 22, 2014).

approved authorization form. Privacy Notice at 2. There are no exceptions. Complaint, ¶37.

Finally, St. Joseph represents and promises that it “safeguards customer information using various tools such as firewalls, passwords and data encryption” and “continually strive[s] to improve these tools to meet or exceed industry standards.” *Id.* Ironically, St. Joseph also promises to “limit access to [its patients’] information to protect against its unauthorized use.” *Id.* Complaint, ¶40.

St. Joseph entered into an express, written contract with Peters when she signed the Privacy Notice, provided St. Joseph with her PII/PHI, and paid her money in exchange for the health care services and data protection services St. Joseph provided or, in this case, promised to provide, but did not. Complaint, ¶34. By its alleged wrongful actions, inaction and/or omissions, and the resulting Data Breach, St. Joseph breached its contract with Peters.

2. Peters properly states her breach of implied contract claim (Count VIII, Complaint, ¶¶111-115).

An implied contract arises from:

[T]he acts and conduct of the parties. Such a contract exists when the facts and circumstances surrounding the parties' relationship imply a mutual intention to contract. Every contract requires a meeting of the minds, but the meeting can be implied from and evidenced by the parties' conduct and course of dealing.

See, e.g., Harrison v. Williams Dental Group, P.C., 140 S.W.3d 912, 916 (Tex. App.-Dallas 2004, no pet.) (citing *Haws & Garrett Gen. Contractors, Inc. v.*

Gorbett Bros. Welding Co., 480 S.W.2d 607, 609 (Tex.1972)). St. Joseph does not dispute that an implied contract exists between the Parties.

The Supreme Court in *Haws & Garrett* looked to what was then tentative § 21 (but ultimately became § 19) of the RESTATEMENT (SECOND) OF CONTRACTS and Professor Williston's treatise on Contracts in discussing how a mutual agreement can be “inferred from the circumstances.” *Haws & Garrett*, 480 S.W.2d at 609. Section 19 of the RESTATEMENT provides that:

- (1) The manifestation of assent may be made wholly or partly by written or spoken words or by other acts or by failure to act.
- (2) The conduct of a party is not effective as a manifestation of his assent unless he intends to engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents.
- (3) The conduct of a party may manifest assent even though he does not in fact assent. In such cases a resulting contract may be voidable because of fraud, duress, mistake, or other invalidating cause.

The Fifth Circuit and the First Court of Appeals have expressly relied on this provision in decisions involving contract formation. *See, e.g., Hollywood Fantasy Corp. v. Gabor*, 151 F.3d 203, 210–11 (5th Cir. 1998); *Karl Rove & Co. v. Thornburgh*, 39 F.3d 1273, 1291–93 (5th Cir. 1994); *Texaco, Inc. v. Pennzoil Co.*, 729 S.W.2d 768, 818 (Tex. App.-Houston [1st Dist.] 1987, writ ref'd n.r.e.).

The holding in *Richardson v. DSW, Inc.*, Case No. 05 C 4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005), a data breach case, is instructive here. There,

the plaintiff used credit and debit cards to purchase shoes from DSW, a retailer. *Id.* at *1. After DSW publicly admitted that customers' credit and debit cards had been stolen from its computer system, plaintiff filed suit against DSW asserting, among other claims, breach of implied contract. *Id.* Despite the fact that plaintiff did not allege her PII had been misused, and despite the fact plaintiff did not suffer any fraudulent charges on her credit or debit cards, the court denied DSW's motion to dismiss, finding plaintiff pled a valid breach of implied contract claim because DSW "not only offered to accept certain forms of non-cash payment in exchange for shoes but also *offered to take reasonable measures to keep this information secure.*" *Id.* at *3-*4 (emphasis added). *See also In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (citing *Anderson v. Hannaford Bros.*, 659 F.3d 151 (1st Cir. 2011)).

In *Anderson*, another data breach case, the First Circuit affirmed the district court's finding that a jury could reasonably find an implied contract existed between the defendant and its customers that defendant would take reasonable measures to protect their financial information. *Id.* at 158. The First Circuit elaborated that "[w]hen a customer uses a credit card in a commercial transaction, she intends to provide the data to the merchant only ... and does not expect—and certainly does not intend—the merchant to allow unauthorized third parties to

access that data.” *Id.* “A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.” *Id.*

The same is no less true here. Pursuant to the Privacy Notice, St. Joseph *offered to take reasonable measures to keep Peters’ PII/PHI secure.* Based on the facts and circumstances surrounding the Parties’ relationship, and even if they did not enter into an express, written contract, in the alternative, and at the very least, they mutually intended to enter, and entered, into a contract for health care services and data protection services as implied from, and evidenced by, their conduct and course of dealing—which St. Joseph breached.

D. Peters properly states her Texas Deceptive Trade Practices-Consumer Protection Act (“DTPA”) claims (Count IX, Complaint, ¶¶116-120).

Peters asserts two DTPA causes of action: (i) violation of §17.50(a)(3) (an unconscionable action or course of action), and (ii) violation of §17.50(a)(1) (employing a false, misleading, or deceptive act or practice—in this case, the acts and practices enumerated in §17.46(b)(5) and (b)(7)).

St. Joseph does not argue that its failure to safeguard and protect Peters’ PII/PHI was not unconscionable. Nor does St. Joseph argue that its conduct did not violate §17.46(b)(5) and (b)(7). Rather, St. Joseph argues that (i) both of Peters’ DTPA claims fail because she does not qualify as a “consumer” under the statute (MTD at 17-19), but alternatively, (ii) even if she does, her §17.50(a)(1)

claims—but not her §17.50(a)(3) claim—fail because Peters fails “to allege damages that resulted from her reliance on Defendants’ statements.” MTD at 20.

St. Joseph cites *McClung v. Wal-Mart*, 866 F. Supp. 306, 308 (N.D. Tex. 1994), for the proposition that Peters is not a consumer because she:

[A]cquired ***health care services*** by purchase; however, the health care services do not form the basis of her complaint. Her complaint arises out of alleged damages resulting from a data breach. As such, Plaintiff does not have “consumer” status in conjunction with the claims asserted.

MTD at 18 (emphasis in original). Contrary to St. Joseph’s assertion, the facts presented here are not analogous to *McClung*. They are remarkably different.

The plaintiff, in *McClung*, bought a telephone, but complained about Wal-Mart’s post-transaction conduct, which plaintiff alleged were “services” to be rendered in connection with his purchase of the telephone. The court held that even if the statutory definition of “services” could be distorted to cover plaintiff’s claims, such “services” were “incident to, rather than in connection with” his telephone purchase. *Id.*, 866 F. Supp. at 309. As such, he was not a “consumer” under the DTPA. *Id.*

Here, on the other hand, Peters did not purchase a good from St. Joseph, but rather, health care services and data protection services. *See, e.g.*, Complaint, ¶¶ 108-10, 113-15, 117 (“Plaintiff and Class Members are “consumers” under the [DTPA], ... *by purchasing health care services and PII/PHI protection services*

from St. Joseph.”) (emphasis added). The PHI/PII protection services St. Joseph failed to provide form the basis of her DTPA claims. *McClung*, 866 F. Supp. at 308 (citations omitted). Peters is a “consumer” under the DTPA.

Regarding her §17.46(b)(5); (b)(7) claims, Peters stands on her Complaint and the damages briefing in her Response to St. Joseph’s Rule 12(b)(1) MTD, which she incorporates in this Response. The notion that Peters did not rely on St. Joseph’s promises to protect her PII/PHI in its Privacy Notice (Complaint, ¶119)—which she was required to sign in conjunction with providing her PII/PHI to St. Joseph—is beyond comprehension.

E. Peters properly states her invasion of privacy claim (Count X, Complaint, ¶¶121-126).

St. Joseph advances two arguments for the dismissal of Peters’ claim for invasion of privacy by public disclosure of private facts; to wit, (i) Peters does not contend St. Joseph publicized her PII/PHI (MTD at 21), and (ii) even if St. Joseph publicized her PII/PHI, St. Joseph publicized it to a single data thief or small group of data thieves.⁶ MTD at 22.

Regarding St. Joseph’s first argument, Peters clearly contends St. Joseph publicized her PII/PHI. *See* Peters’ compendium of Complaint allegations asserting St. Joseph’s disclosure of her PII/PHI at Section H, *infra*, which Peters

⁶ How St. Joseph already knows that it published Peters’ and Class Members’ PII/PHI only to “a single person or small group” of data thieves is an interesting fact question that awaits discovery.

incorporates by reference. *See also* Complaint, ¶124 (“St. Joseph’s above-described wrongful dissemination of Plaintiff’s and Class Members’ PII/PHI *into the public domain* is not of a legitimate public concern ...”), ¶125 (“St. Joseph intentionally invaded Plaintiff’s and Class Members’ privacy by *disseminating their PII/PHI to the world* by repeatedly failing and refusing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the security and confidentiality of their PII/PHI.”) (emphasis added).

Invasion of privacy centers on the “publicity” of a person’s confidential and private information without a legitimate reason for doing so. *See, e.g., Star-Telegram, Inc. v. Doe*, 915 S.W.2d 471, 473-74 (Tex. 1995). “Publicity” is the communication of a matter to the public at large or disseminated to so many people that it becomes public knowledge. *Indus. Found. v. Texas Indus. Acc. Bd.*, 540 S.W.2d 668, 683-84 (Tex. 1976), *cert. denied*, 430 U.S. 931 (1977).

In *Industrial Found.*, the Texas Supreme Court held that where government records containing private information were opened to public inspection, the information was sufficiently “publicized” to support an invasion of privacy claim:

To hold otherwise would be to deny an individual any protectable privacy interest in private information disclosed to a governmental unit, if such information would otherwise be “public information.”

Id. at 684. Thus, the common law tort of public disclosure of private facts simply requires “a communication that reaches, or is sure to reach, the public.” RESTATEMENT §652D, Cmt. a (emphasis added); *see also Biederman's of Springfield, Inc. v. Wright*, 322 S.W.2d 892, 898 (Mo. 1959). The likelihood of widespread dissemination can be inferred from the medium employed by the defendant for the particular publication (*see, e.g., Barber v. Time, Inc.*, 159 S.W.2d 291 (Mo. 1942); *Williams v. KCMO Broad. Div. Meredith Corp.*, 472 S.W.2d 1 (Mo. App. 1971)), or from the defendant’s action in making private information available to the public where further dissemination is likely.

Here, and setting aside the fact that Peters alleges St. Joseph disseminated her PII/PHI *into the public domain* and *to the world* (Complaint, ¶¶124, 125), the likelihood of the widespread dissemination of Peters’ PII/PHI can be inferred from the medium employed by St. Joseph—in this case, the worldwide web.

F. Peters properly alleges emotional distress.

Peters technically pleads emotional distress as a type of injury or harm she suffered as a result of the Data Breach (*see, e.g., Complaint*, ¶148), rather than as a formal cause of action. That said, St. Joseph correctly states the elements of an emotional distress claim under Texas law. MTD at 22. However, in disavowing the claim, St. Joseph ignores Peters’ plain allegations that it acted intentionally

and/or recklessly in failing to safeguard and protect Peters’ and Class Members’ PII/PHI. Complaint, ¶¶ 2, 4, 5, 52, 76, 77, 118, 122, 125, 136, and 150.

The notion that St. Joseph’s intentional and/or reckless failure to safeguard and protect Peters’ and Class Members’ PII/PHI that, in turn, caused the dissemination of their PII/PHI to the world and the resulting consequences was not extreme and outrageous strains credulity. St. Joseph concedes Peters suffered emotional distress as a result. MTD at 22-23. Should the Court view Peters’ emotional distress as a formal cause of action, it should not be dismissed.

G. Peters properly states her claims for negligence (Count V, Complaint, ¶¶ 91-100) and negligence *per se* (Count VI, Complaint, ¶¶ 101-105).

Here, St. Joseph simply argues that Peters “fails to state a claim for negligence and/or negligence *per se*, pursuant to HIPAA, upon which relief may be granted.” MTD at 23-24. Even if St. Joseph’s argument is accurate—which it is not—her negligence and negligence *per se* claims do not fail because they are not predicated on HIPAA alone, but also on:

Texas common law, ... because it was reasonably foreseeable to St. Joseph under the circumstances that a data breach in its computer system was likely to occur St. Joseph’s duty also arises from the PII/PHI security obligations expressly imposed upon it by, *inter alia*, HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed.”

See Complaint, ¶92 (negligence), ¶¶102-104 (negligence *per se*).

Peters does not dispute there is no private cause of action under HIPAA, nor does she seek to impose one. HIPAA, on the other hand, can set the standard for common law negligence-based claims—which Peters alleges here. Notwithstanding the holding in *Johnson v. Sawyer* (MTD at 24), “[t]he violation of federal statutes and regulations is commonly given negligence per se effect in state tort proceedings.” *Grable & Sons Metal Prod., Inc. v. Darue Eng. & Mfg.*, 545 U.S. 308, 318 (2005) (citing RESTATEMENT (THIRD) TORTS § 14, cmt. a).

Thus, courts have found viable state law claims where violation of the HIPAA privacy rule was an element of the cause of action. *See, e.g., R.K. v. St. Mary’s Medical Center, Inc.*, 735 S.E.2d 715, 723 (W.Va. 2012) (identifying several courts where HIPAA supplied the standard of care and/or established negligence *per se*); *I.S. v. Washington University*, No. 4:11CV235SNLJ, 2011 WL 2433585, at *2 (E. D. Mo. June 14, 2011) (negligence claim “may stand as a state claim for negligence *per se* despite its exclusive reliance upon HIPAA”). The same is true here.

H. Peters properly states her claims for St. Joseph’s violations of the Texas Medical Practice Act (Count III, Complaint, ¶¶ 82-85), violations of the Texas Hospital Licensing Law (Count IV, Complaint, ¶¶ 86-90), and breach of fiduciary duty (Count XI, Complaint, ¶¶ 127-137).

This is St. Joseph’s only attack on Peters’ Texas Medical Practice Act and Texas Hospital Licensing Law claims, and the only attack on Peters’ breach of fiduciary duty claim other than the “no damages” argument (Section B, *infra*).

Here, St. Joseph simply argues that since these claims require a defendant to disclose confidential information, they should be dismissed because “Plaintiff does not allege that Defendants disclosed her PII/PHI.” MTD at 25.

St. Joseph is wrong; it overlooks multiple allegations that it disclosed Peters’ and Class Members’ PII/PHI without their authorization. *See, e.g.*, Complaint, ¶48 (“[I]f a Class Member is victimized by a phishing scam fueled by *the PII/PHI disclosed by St. Joseph in the Data Breach*, he or she will lose the AllClear ID ‘protection services’”); ¶51 (“St. Joseph flagrantly and/or negligently disregarded and/or violated Plaintiff’s and Class Members’ privacy rights, and harmed them in the process, *by not obtaining their prior written consent to disclose their PII/PHI* to any other person or organization and/or for any purpose other than the persons, organizations and purposes listed in the Privacy Notice.”); *see also* ¶¶ 19, 90, 100, 105, 120, 126, 137, and 141 (referencing St. Joseph’s “improper disclosure of her PII/PHI without authorization” and St. Joseph’s “unauthorized disclosure of Plaintiff’s and Class Members’ ‘health care information’ (*i.e.*, their PII/PHI) to unauthorized parties”); and ¶¶54, 57, 59, 77, 85, and 90 (“St. Joseph’s failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ PII/PHI—*directly and/or*

proximately caused the Data Breach, [and] caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI.") (emphasis added).

I. Peters properly states her breach of confidentiality claim (Count XII, Complaint, ¶¶ 138-141).

Peters concedes a common law claim for breach of confidentiality—also known as “breach of confidence”—has not been formally recognized by Texas courts, but advocates, in good faith, for the recognition of a common law tort similar to the tort recognized by the Ohio Supreme Court in *Biddle v. Warren Gen. Hosp.*, 715 N.E.2d 518, 523 (Ohio 1999) (recognizing an independent tort for the unauthorized, unprivileged disclosure of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship).⁷

Here, Peters alleges St. Joseph disclosed her PHI to third parties without authorization. *See supra*. St. Joseph admitted in its Data Breach notification letter (Complaint, Exhibit A) that Peters' PHI was disclosed in the Data Breach without her authorization—which constitutes breach of confidence at common law.

WHEREFORE, Plaintiff Beverly T. Peters, on behalf of herself and Class Members, respectfully requests this Court to (i) deny St. Joseph's Rule 12(b)(6) motion to dismiss, and (ii) grant her such other and further relief to which she is justly entitled.

⁷ See also Brian C. Murchison, *Reflections on Breach of Confidence from the U.S. Experience*, 15 Media & Arts L. Rev. 295 (2010); Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982).

Date: August 29, 2014

Respectfully submitted,

/s/ Richard L. Coffman

Richard L. Coffman

THE COFFMAN LAW FIRM

Texas Bar No. 04497460

Federal Bar No. 12055

505 Orleans St., Ste. 505

Beaumont, TX 77701

Telephone: (409) 833-7700

Facsimile: (866) 835-8250

Email: rcoffman@coffmanlawfirm.com

Mitchell A. Touns

WELLER, GREEN, TOUPS & TERRELL, LLP

Texas Bar No. 20151600

Federal Bar No. 2457

2615 Calder Ave., Suite 400

Beaumont, TX 77702

Telephone: (409) 838-0101

Facsimile: (409) 838-6780

Email: matouns@wgttlaw.com

Jason Webster

THE WEBSTER LAW FIRM

Texas Bar No. 24033318

Federal Bar No. 568715

6200 Savoy, Suite 515

Houston, TX 77036

Telephone: (713) 581-3900

Facsimile: (713) 409-6464

Email: jwebster@thewebsterlawfirm.com

CERTIFICATE OF SERVICE

I certify that a true and correct copy of Plaintiff's Response in Opposition to Defendants' Rule 12(b)(6) Motion to Dismiss was served on the following counsel of record, via the Court's ECF System, on August 29, 2014.

/s/ Richard L. Coffman
Richard L. Coffman

Kent Adams
Kristie Johnson
LEWIS BRISBOIS BISGAARD & SMITH, LLP
Weslayan Tower, Suite 1400
24 East Greenway Plaza
Houston, Texas 77046
Telephone: (713) 659-6767
Facsimile: (713) 759-6830
Email: Kent.adams@lewisbrisbois.com
Email: Kristie.johnson@lewisbrisbois.com

ATTORNEYS FOR DEFENDANTS